CLAIMS

1. A method of decrypting content stored on a terminal, the method comprising

obtaining a license comprising a content decryption key and a set of binding attributes, the attributes including a public key;

establishing communication link between the terminal and at least one other terminal; and

receiving digitally signed data on the communication link at the terminal from the other terminal;

verifying at the terminal the digitally signed data utilizing the said public key; and wherein

the terminal in response to verification of the digitally signed data uses the content decryption key to decrypt the content.

2. A method as claimed in Claim 1, comprising:

encrypting at least the content decryption key.

3. A method as claimed in Claim 2, wherein:

encryption is performed using a public key of an asymmetric key pair such that decryption of the content decryption key is carried out using a private key of the asymmetric key pair.

4. A method as claimed in Claim 3, wherein:

the private key is stored in a tamperproof and secure location.

5. A method as claimed in Claim 4, wherein:

the secure location comprises a security element.

6. A computer program comprising:

executable code which executes when loaded on a computer, to perform the method according to Claim 1.

7. A computer program comprising:

executable code which executes when loaded on a computer, to perform the method according to Claim 2.

8. A computer program comprising:

executable code which executes when loaded on a computer, to perform the method according to Claim 3.

9. A computer program comprising:

executable code which executes when loaded on a computer, to perform the method according to Claim 4.

10. A computer program comprising:

executable code which executes when loaded on a computer, to perform the method according to Claim 5.

11. A program as claimed in Claim 6, stored in a computer readable medium.

12. A program as claimed in Claim 7, stored in a computer readable medium.

13. A program as claimed in Claim 8, stored in a computer readable medium.

14. A program as claimed in Claim 9, stored in a computer readable medium.

15. A program as claimed in Claim 10, stored in a computer readable medium.

16. A terminal which renders encrypted content comprising:

a storage for the encrypted content and a license, the license containing a content decryption key and a set of binding attributes, the attributes including a public key;

a protected processing environment;

a network interface which establishes a communication link between the terminal and at least one other terminal and which delivers digitally signed data received from the other terminal to the protected processing environment; and wherein upon successful verification of the digitally signed data, with the public key, the protected processing environment decrypts the encrypted content using the content decryption key.

17. A terminal as claimed in Claim 16, comprising:

a tamperproof and secure storage for a private key of an asymmetric key pair; and wherein

the protected processing environment decrypts at least the content decryption key, the content decryption key having been encrypted using a public key of the asymmetric key pair.

18. A terminal as claimed in Claim 17, wherein:

the storage is provided by a security element.

19. A terminal as claimed in Claim 16, wherein:

the digitally signed data is delivered to the storage.

20. A terminal as claimed in Claim 17, wherein:

the digitally signed data is delivered to the storage.

21. A terminal as claimed in Claim 18, wherein:

the digitally signed data is delivered to the storage.

22. A terminal as claimed in Claim 16, wherein:

the protected processing environment verifies the digitally signed data.

23. A terminal as claimed in Claim 17, wherein:

the protected processing environment verifies the digitally signed data.

24. A terminal as claimed in Claim 18, wherein:

the protected processing environment verifies the digitally signed data.

25. A terminal as claimed in Claim 19, wherein:

the protected processing environment verifies the digitally signed data.

26. A terminal as claimed in Claim 20, wherein:

the protected processing environment verifies the digitally signed data.

27. A terminal as claimed in Claim 21, wherein:

the protected processing environment verifies the digitally signed data.

28. A terminal as claimed in Claims 16, wherein:

the network interface issues a request to the other terminal to provide the digitally signed data.

29. A terminal as claimed in Claims 17, wherein:

the network interface issues a request to the other terminal to provide the digitally signed data.

30. A terminal as claimed in Claims 18, wherein:

the network interface issues a request to the other terminal to provide the digitally signed data.

31. A terminal as claimed in Claims 19, wherein:

the network interface issues a request to the other terminal to provide the digitally signed data.

32. A terminal as claimed in Claims 20, wherein:

the network interface issues a request to the other terminal to provide the digitally signed data.

33. A terminal as claimed in Claims 21, wherein:

the network interface issues a request to the other terminal to provide the digitally signed data.

34. A terminal as claimed in Claims 22, wherein:

the network interface issues a request to the other terminal to provide the digitally signed data.

35. A method for creating a license which facilitates decryption of content on a terminal, the method comprising:

appending a set of binding attributes to a content decryption key wherein the binding attributes include attributes obtained from a trusted storage.

36. A method as claimed in Claim 35 wherein:

the binding attributes from the trusted storage comprise a public key certificate of a licensee with a corresponding private key being held on another terminal.

37. A method as claimed in Claim 36, comprising encrypting at least the content decryption key.

38. A method as claimed in Claim 37, comprising:

distributing to the terminal a decryption key for decrypting the encrypted content decryption key.

39. A method as claimed in any one of Claim 36, wherein:

a plurality of binding attributes each having a respective public key certificate of a licensee are appended to the content decryption key.

40. A method as claimed in any one of Claim 37, wherein:

a plurality of binding attributes each having a respective public key certificate of a licensee are appended to the content decryption key.

41. A method as claimed in any one of Claim 38, wherein:

a plurality of binding attributes each having a respective public key certificate of a licensee are appended to the content decryption key.

42. A computer program comprising:

executable code which is executed when loaded on a computer, to perform the method according to Claim 36.

43. A computer program comprising:

executable code which is executed when loaded on a computer, to perform the method according to Claim 37.

44. A computer program comprising:

executable code which is executed when loaded on a computer, to perform the method according to Claim 38.

45. A computer program comprising:

executable code which is executed when loaded on a computer, to perform the method according to Claim 39.

46. A computer program comprising:

executable code which is executed when loaded on a computer, to perform the method according to Claim 40.

47. A computer program comprising:

executable code which is executed when loaded on a computer, to perform the method according to Claim 41.

48. A program as claimed in Claim 42, stored in a computer readable medium.

49. A program as claimed in Claim 43, stored in a computer readable medium.

50. A program as claimed in Claim 44, stored in a computer readable medium.

51. A program as claimed in Claim 45, stored in a computer readable medium.

52. A program as claimed in Claim 46, stored in a computer readable medium.

53. A program as claimed in Claim 47, stored in a computer readable medium.

54. A method of distributing encrypted content to a rendering machine comprising:

delivering encrypted content and a license relating thereto to a rendering machine, the license containing binding attributes corresponding to a user identity; and

requesting authentication of the attributes by a personal trusted device.

55. A method as claimed in Claim 54, comprising:

storing securely a license decryption key on the rendering machine.

56. A method as claimed in Claim 55, wherein:

the license decryption key is in a protected processing environment and is a private key with a corresponding public key being used to encrypt the license.

57. A method as claimed in Claims 54, wherein:

the binding attributes comprise a public key certificate of a user.

58. A method as claimed in Claims 55, wherein:

the binding attributes comprise a public key certificate of a user.

59. A method as claimed in Claims 56, wherein:

the binding attributes comprise a public key certificate of a user.

60. A method as claimed in Claim 52, wherein:

the request for authentication of the attributes comprises a request to provide digitally signed data.

61. A method as claimed in Claim 58, wherein:

the request for authentication of the attributes comprises a request to provide digitally signed data.

62. A method as claimed in Claim 59, wherein:

the request for authentication of the attributes comprises a request to provide digitally signed data.

63. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables to carry out the method according to Claim 54.

64. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables to carry out the method according to Claim 55.

65. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables to carry out the method according to Claim 56.

66. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables to carry out the method according to Claim 57.

67. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables in accordance with the code to carry out the method according to Claim 58.

68. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables to carry out the method according to Claim 59.

69. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables to carry out the method according to Claim 60.

70. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables to carry out the method according to Claim 61.

71. A computer program comprising:

executable code which executes when loaded on a computer, wherein the computer operables to carry out the method according to Claim 62.

72. A terminal which renders encrypted content comprising:

a storage for the encrypted content and a license, the license containing a content decryption key and a set of binding attributes, the attributes including a public key;

a protected processing environment;

a communication link between the terminal and at least one other terminal which delivers digitally signed data from the other terminal to the terminal;

a digital rights management engine disposed in a non-secure part of the terminal; and

a digital rights management agent disposed within the protected processing environment which verifies if the digitally signed data is signed by a licensee of the encrypted content and upon verification, uses the content decryption key to decrypt the encrypted content.

73. A terminal in accordance with Claim 72 wherein:

the storage is unprotected; and

the digital rights management engine decrypts the set of binding attributes to determine if the encrypted content is licensed to the licensee to be decrypted and if the encrypted content is authorized to be decrypted signals the digital rights management engine to render the content.

74. A terminal in accordance with Claim 73 wherein:

the decryption key is encrypted; and

the digital rights management agent obtains the binding attributes and obtains the content decryption key by using a private protected processing environment key to decrypt the encrypted decryption key.

75. A terminal in accordance with Claim 72 wherein:

an encrypted part of the license includes a user identity certificate issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

76. A terminal in accordance with Claim 72 wherein:

an encrypted part of the license includes a user identity certificate issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

77. A terminal in accordance with Claim 74 wherein:

an encrypted part of the license includes a user identity certificate issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

78. A terminal in accordance with Claim 72 wherein:

an encrypted part of the license includes a URL which is an address at which a user identity certificate was issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

79. A terminal in accordance with Claim 73 wherein:

an encrypted part of the license includes a URL which is an address at which a user identity certificate was issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

80. A terminal in accordance with Claim 74 wherein:

an encrypted part of the license includes a URL which is an address at which a user identity certificate was issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

81. A terminal in accordance with Claim 75 wherein:

an encrypted part of the license includes a URL which is an address at which a user identity certificate was issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.

82. A terminal in accordance with Claim 76 wherein:

an encrypted part of the license includes a URL which is an address at which a user identity certificate issued and digitally signed by a certification authority may be obtained which permits a licensor of the content to establish a level of trust in a licensee of the content.

83. A terminal in accordance with Claim 77 wherein:

an encrypted part of the license includes a URL which is an address at which a user identity certificate was issued and digitally signed by a certification authority which permits a licensor of the content to establish a level of trust in a licensee of the content.